In the Claims:

1. (Original) A random number source comprising:

a ring oscillator generating an internal clock signal having random phase noise;

a first linear feedback shift register connected to said ring oscillator and comprising a plurality of taps;

a counter connected to at least one first tap of said first linear feedback shift register for generating a count signal;

a feedback bit controller connected to a second tap of said first linear feedback shift register for generating a random feedback bit for a time based upon the count signal; and

a second linear feedback shift register connected to said feedback bit controller for generating a random number based upon the random feedback bit.

2. (Currently amended) A random number source according to Claim 1 further comprising a system clock connected to said ring oscillator, said feedback bit controller and said second ~~first~~ linear feedback shift register.

3. (Original) A random number source according to Claim 2 wherein a frequency of the internal clock signal is greater than a frequency of a system clock signal.

4. (Original) A random number source according to Claim 2 wherein a frequency of the internal clock signal is not an integer multiple of a frequency of a system clock signal.

5. (Original) A random number source according to Claim 1 wherein said second linear feedback shift register comprises a feedback path; and wherein said feedback bit controller is connected to the feedback path for inputting the random feedback bit into the feedback path.

6. (Original) A random number source according to Claim 5 wherein said counter defines the time that the feedback bit is input into the feedback path based upon a count cycle of said counter.

7. (Original) A random number source according to Claim 6 wherein the time is random for each count cycle.

8. (Original) A random number source according to Claim 1 wherein said first linear feedback shift register comprises n bits, and said second linear feedback shift register comprises m bits, with n being between 20 and 60, and m being between 40 and 80.

9. (Original) An encryption device comprising:

a random number source for generating a random number and comprising

a ring oscillator generating an internal clock signal having random phase noise,

a first linear feedback shift register connected to said ring oscillator and comprising a plurality of taps,

a counter connected to at least one first tap of said first linear feedback shift register for generating a count signal,

a feedback bit controller connected to a second tap of said first linear feedback shift register for generating a random feedback bit for a time based upon the count signal, and

a second linear feedback shift register connected to said feedback bit controller for generating the random number based upon the random feedback bit; and

a cryptographic key generator connected to said random number source and generating an output signal based upon the random umber.

10. (Original) An encryption device according to Claim 9 wherein the output signal includes at least one of random cryptographic keys, randomization vectors for an initial state of a cryptographic session, and initialization vectors for a cryptographic session.

11. (Currently amended) An encryption device according to Claim 9 further comprising a system clock connected to said ring oscillator, said feedback bit

controller and said second ~~first~~ linear feedback shift register.

12. (Original) An encryption device according to Claim 11 wherein a frequency of the internal clock signal is greater than a frequency of a system clock signal.

13. (Original) An encryption device according to Claim 11 wherein a frequency of the internal clock signal is not an integer multiple of a frequency of a system clock signal.

14. (Original) An encryption device according to Claim 9 wherein said second linear feedback shift register comprises a feedback path; and wherein said feedback bit controller is connected to the feedback path for inputting the random feedback bit into the feedback path.

15. (Original) An encryption device according to Claim 14 wherein said counter defines the time that the feedback bit is input into the feedback path based upon a count cycle of said counter.

16. (Original) An encryption device according to Claim 15 wherein the time is random for each count cycle.

17. (Original) An encryption device according to Claim 9 wherein said first linear feedback shift register comprises n bits, and said second linear feedback shift

register comprises m bits, with n being between 20 and 60, and m being between 40 and 80.

18. (Original) An encryption device according to Claim 9 further comprising a portable housing containing said random number source and said cryptographic key generator.

19. (Original) An electronic device comprising:

a random number source for generating a random number and comprising

a ring oscillator generating an internal clock signal having random phase noise,

a first linear feedback shift register connected to said ring oscillator and comprising a plurality of taps,

a counter connected to at least one first tap of said first linear feedback shift register for generating a count signal,

a feedback bit controller connected to a second tap of said first linear feedback shift register for generating a random feedback bit for a time based upon the count signal, and

a second linear feedback shift register connected to said feedback bit controller for generating the random number based upon the random feedback bit; and

other circuitry connected to said random number source for performing a desired operation based on the random number.

20. (Original) An electronic device according to Claim 19 wherein the desired operation is a smart card operation.

21. (Original) An electronic device according to Claim 19 wherein the desired operation is an electronic gaming operation.

22. (Currently amended) An electronic device according to Claim 19 further comprising a system clock connected to said ring oscillator, said feedback bit controller and said second ~~first~~ linear feedback shift register.

23. (Original) An electronic device according to Claim 22 wherein a frequency of the internal clock signal is greater than a frequency of a system clock signal.

24. (Original) An electronic device according to Claim 22 wherein a frequency of the internal clock signal is not an integer multiple of a frequency of a system clock signal.

25. (Original) An electronic device according to Claim 19 wherein said second linear feedback shift register comprises a feedback path; and wherein said feedback bit controller is connected to the feedback path for inputting the random feedback bit into the feedback path.

26. (Original) An electronic device according to Claim 25 wherein said counter defines the time that the feedback bit is input into the feedback path based upon a count cycle of said counter.

27. (Original) An electronic device according to Claim 26 wherein the time is random for each count cycle.

28. (Original) An electronic device according to Claim 19 wherein said first linear feedback shift register comprises n bits, and said second linear feedback shift register comprises m bits, with n being between 20 and 60, and m being between 40 and 80.

29. (Currently amended) An electronic ~~encryption~~ device according to Claim 19 further comprising a portable housing containing said random number source and said other circuitry.

30. (Original) A method for generating a random number comprising:

generating an internal clock signal having random phase noise using a ring oscillator;

providing the internal clock signal to a first linear feedback shift register;

generating a count signal using a counter connected to at least one first tap of the first linear feedback shift register;

generating a random feedback bit for a time based upon the count signal using a feedback bit controller connected to a second tap of the first linear feedback shift register; and

generating the random number based upon the random feedback bit using a second linear feedback shift register connected to the feedback bit controller.

31. (Original) A method according to Claim 30 further comprising using the random number in a cryptographic key generator.

32. (Original) A method according to Claim 30 further comprising using the random number in a smart card.

33. (Original) A method according to Claim 30 further comprising using the random number in an electronic gaming device.

34. (Currently amended) A method according to Claim 30 further comprising providing system clock signals to the ring oscillator, the feedback bit controller and the second ~~first~~ linear feedback shift register.

35. (Original) A method according to Claim 34 wherein a frequency of the internal clock signal is greater than a frequency of a system clock signal.

36. (Original) A method according to Claim 34 wherein a frequency of the internal clock signal is not an integer multiple of a frequency of a system clock signal.

37. (Original) A method according to Claim 30 wherein the second linear feedback shift register comprises a feedback path; and further comprising inputting the random feedback bit into the feedback path.

38. (Original) A method according to Claim 37 wherein the counter defines the time that the feedback bit is input into the feedback path based upon a count cycle of the counter.